

TESTIMONY OF ELAINE DEZENSKI
ACTING ASSISTANT SECRETARY
BORDER AND TRANSPORTATION DIRECTORATE
DEPARTMENT OF HOMELAND SECURITY
BEFORE
THE HOUSE HOMELAND SECURITY SUBCOMMITTEE ON
ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
“ENSURING THE SECURITY OF AMERICAN BORDERS THROUGH BIOMETRIC
PASSPORTS AND OTHER IDENTIFICATION DOCUMENTS”

June 22, 2005

Chairman Lungren, Ranking Member Sanchez and other distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the approach that the Department of Homeland Security (DHS) is taking in our efforts to improve the security of the United States by the use of biometrics in travel documents.

DHS is committed to secure travel and our recent decision to clarify the deadline for Visa Waiver Program (VWP) countries to produce “e-passports” is emblematic of how the Department and the State Department (DOS) are working to keep our borders safe but open for legitimate travelers.

Programs such as the VWP advance our shared goals of protecting travel and preserving the integrity of our borders – while stopping terrorists and those who mean us harm. DHS is committed to continuing the VWP while strengthening it by closing down vulnerabilities such as fraudulent passport use. One means to do this is through the requirement that biometric information be incorporated into travel documents.

Biometrics are the way forward in enhancing security by helping us to deprive potential terrorists of a tool they use to threaten our country and other countries around the world: the ability to cross our borders using false documents and violate our immigration laws without detection. Biometric identifiers protect our visitors by making it extremely difficult for anyone else to assume their identities should their travel documents be stolen or duplicated. The use of biometric identifiers gives governments an increased security capability and a foundation it can build on over time. Properly used, biometrics have been shown to be highly effective in verifying identity.

The U.S. Congress mandated in the Enhanced Border Security and Visa Entry Reform Act of 2002, as amended, that any passport issued on or after October 26, 2005, and used for VWP travel to the United States, must incorporate biometric identifiers that meet internationally accepted standards established by ICAO. The Administration's recently announced policy furthers the intent of the statute by providing for the adoption of biometrics and strengthening the overall management of this important program.

More specifically, we, in consultation with Congress and the Department of State, have established policy that requires VWP countries to begin producing machine-readable passports with digital photographs on the passport's data page by October 26, 2005. Digital photographs provide more security against counterfeiting than traditional photographs. Digital photos can be electronically stored and accessed, making it easier to verify whether the individual currently presenting the passport is the same person to whom the passport was issued. In addition, DHS has established a policy requiring all VWP countries to produce passports with an integrated circuit chip, known as "*e-passports*," capable of storing biographic information from the data page of a passport, a digitized photograph, and other biometric information no later than October 26, 2006. This information will allow us to achieve a new level of identity authentication.

The effect of this policy is that VWP countries will be required to issue passports that have at a minimum a digital photo by this October and that a VWP traveler to the United States must present a machine-readable passport which includes a digital photograph to enter the United States. These requirements apply only to passports issued on or after October 26, 2005. Valid passports issued before October 26, 2005, will still be valid for travel under the VWP, provided that they are machine-readable. We believe the vast majority of the VWP nations will be in compliance with the digital photo requirement by October.

The Department recognizes that some countries are very close or have even launched their production of "*e-passports*." Obviously, those countries will also be in compliance with the upcoming deadline. In order to facilitate compliance with e-passport requirements, we will work with each country on a bi-lateral basis with regard to biometrics as well as other security provisions required of VWP countries. Further, DHS will create a validation process for VWP countries to test their biometric passports prior to issuance. In support of this effort, DHS will host a technical conference this summer to address interoperability issues with reader technology

and with U.S. passport technology. DOS is leading the U.S. effort in production of e-passport for our own citizens.

In further steps forward on “*e-passports*,” DHS and DOS are conducting a “live test” with the governments of Australia and New Zealand. The “live test” began last week at Los Angeles International Airport and at the Sydney Airport in Australia, and will continue throughout the summer. Airline crew and officials from United Airlines, Air New Zealand and Qantas Airlines have volunteered to use the e-passport when arriving at either airport. Their participation will enable DHS to further test operations, equipment and software needed to read and verify the information contained in an e-passport.

Finally, VWP countries will be held to several measures concerning lost and stolen passports such as -- reporting all lost and stolen passports to INTERPOL and DHS, as quickly as possible; sharing information on trends and analysis of lost and stolen passports; and providing detailed information on passport security features.

The progress made toward the “*e-passport*” is a milestone in our global path to secure and streamlined travel for VWP nationals. We appreciate the cooperation of our international partners and the effort they have put forth in this very serious matter.

Mr. Chairman and Members of the Subcommittee, I want to thank you for the opportunity to present this testimony today. I would be pleased to respond to any questions that you might have at this time.